UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,445	12/12/2003	Hamdy Soliman	NMTECH13,CIP3	2018

30996 7590 04/29/2008

ROBERT W. BECKER & ASSOCIATES
707 HIGHWAY 333
SUITE B
TIJERAS, NM 87059-7507

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/735,445	SOLIMAN, HAMDY	
	Examiner	Art Unit	
	ABDULHAKIM NOBAHAR	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-14* is/are rejected.

7)☒ Claim(s) *4* is/are objected to.

8)☒ Claim(s) *15-29* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

Restriction to one of the following inventions is required under 35 U.S.C. 121:

Group I. Claims 1-15, drawn to "a method for providing secure information by regenerating a new encryption key", classified in class 380, subclass 44.

Group II. Claims 16-20, drawn to "a method for authenticating one system node to another system node", classified in class 713, subclass 169.

Group III. Claims 21 and 22, drawn to "a method for validating data by comparing the decrypted data with a data record in a destination node", classified in class 713, subclass 161.

Group IV. Claims 23-29, drawn to "a method for synchronizing one node to another node by aligning the authentication keys of a user and a central authority node", classified in class 380, subclass 260.

The inventions are distinct, each from the other because of the following reasons:

Inventions of Group I, Group II, Group III and Group IV are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention Group I has a separate utility such as generating a new encryption key based on an encryption key, an encrypted data and a hash vector. The

invention Group II has a utility for generating an encryption key at a node by starting a daemon at each node to regenerating a new authentication key with an authentication key, an auxiliary key, and a hash vector based upon an authentication key, and maintaining a corresponding number-regeneration-counter at each node. The invention Group III has a utility that compares a decrypted received data with a data record. The invention Group IV has a utility for comparing a central authority authentication key number regeneration count to a user authentication key number regeneration count. Each of the aforementioned utility of each invention is different from the utility of any other invention and has nothing to do with the other inventions. See MPEP § 806.05(d).

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II, III, or IV, restriction for examination purposes as indicated is proper.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

During a telephone conversation with Mr. Robert W. Becker, Registration Number 26,255, the applicant's representative, on April 17, 2008 a provisional election was made with traverse to prosecute the invention of Group I, claims 1-15. Applicant in replying to this office action must make affirmation of this election. Claims 21-29 are

withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claim Objections

Claims 1, 6-10 are objected to because of the following informalities:

Claim 1 recites "regenerating a new encryption key with an encryption key, encrypted data, and a hash vector based upon an encryption key." It should be rewritten to recites "regenerating a new encryption key with an encryption key, an encrypted data, and a hash vector based upon the encryption key."

This correction should be applied to all other claims as well.

Claims 1, 8, 10 and 15 in preamble recite "A method of providing secure information, the method comprising", but there is no limitation in the claims to provide secure information. The claims limitations provide for regenerating an encryption key. Therefore, the claims limitations in these claims are not for what the invention is intended for.

Claim 6 and 9, in line 3 and line 4, respectively, recite "the range [1, t-1]", where the t value and type have not been specified.

Claim 7, in line 4 recites "and a received cipher" which should be changed to "and a received cipher record" to be consistent with the specification and to make the claim clearer.

Claim 8, in line 3 recites "with n tracks of parallel encryption" which should be changed to "with n tracks of parallel encryption operation (or cryptographic operation)."

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8, in line 3 recites "encrypting n tracks of data records with n tracks of parallel encryption" which is an unclear statement and makes the claim indefinite.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3 and 5-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Meaden (4,642,793).

As per claim 1, Meaden discloses:

A method of providing secure information, the method comprising regenerating a new encryption key with an encryption key, encrypted data, and a hash vector based upon an encryption key (see abstract, col. 2, line 64+ and Fig. 1, where the feedback hashed data F which corresponds to the recited hash vector, the encryption key K and a data are being used to generate an output signal which corresponds to the recited a

new encryption key; col. 2, lines 20-22 and col. 2, line 39+, where the input data is applied to a data selector circuit and the output which corresponds to the recited encrypted data is used for the generation of the signal).

As per claim 2, Meaden discloses:

The method of claim 1 wherein the step of regenerating a new encryption key with an encryption key, encrypted data, and a hash vector based upon an encryption key comprises performing byte addition of an encryption key, encrypted data, and a hash vector based upon an encryption key (see col. 2, lines 17-36 and col. 2, line 67-col. 3, line 5, where the byte combination corresponds to the recited byte addition).

As per claim 3, Meaden discloses:

The method of claim 1 further comprising the step of hashing a hash vector based upon an encryption key (see col. 2, line 67-col. 3, line 5, where the feedback hashed signal F is hashed using the hashing key K).

As per claim 5, Meaden discloses:

The method of claim 1 wherein the step of regenerating a new encryption key with an encryption key, encrypted data, and a hash vector based upon an encryption key comprises:

selecting a previously encrypted data record (col. 2, line 67+ and Fig. 1, where the feedback hashed signal F corresponds to the recited previously encrypted data; and

regenerating a new encryption key with an encryption key, selected encrypted data, and a hash vector based upon an encryption key (see claim 1 rejection above).

As per claim 6, Meaden discloses:

The method of claim 5 wherein the step of selecting a previously encrypted data record comprises:

randomly selecting an index from the range [1, t-1] using a byte of an encryption key as a seed of random generation; and

selecting the previously encrypted data record corresponding to the selected index. See col. 3, lines 18-43, where position of bytes corresponds to the recited index and the operation for transformation of bytes for hashing the data into the output feedback hashed signal F is an equivalent operation to the operation recited in the limitations of this claim.

As per claim 7, Meaden discloses:

The method of claim 1 wherein the step of regenerating a new encryption key with an encryption key, encrypted data, and a hash vector based upon an encryption key comprises regenerating a new encryption key with an encryption key, previously encrypted data, a hash vector based upon an encryption key, and a received cipher (see claim 1 rejection above and further Fig. 1 illustrates that another branch of data corresponding to the recited received cipher outputted from gate 25 is inputted to Mx 39).

As per claim 8, Meaden discloses:

A method of providing secure information, the method comprising the steps of:

generating n encryption keys (see Fig. 1, where one hashed signal H is generated which corresponds to the recited one encryption key);

encrypting n tracks of data records with n tracks of parallel encryption (see Fig. 1 which depicts the transformation one data record D, 10, corresponding to one encrypting track of data record); and

regenerating an encryption key with an encryption key, a hash vector based upon an encryption key, and selected encrypted data (see rejection of claim 1 above for the rejection of similar elements).

As per claim 9, this claim is rejected as applied to the like elements of claim 6.

As per claim 10, Meaden discloses:

A method of providing secure information, the method comprising the steps of:

encrypting a data record with a hash vector based upon an encryption key (see Fig. 1, block 30, where the data is going through a hashing circuit and encrypted by hashing encryption key K);

regenerating an encryption key with an encryption key and encrypted data (see Fig. 1, transformer 13 regenerate the signal H corresponding to the recited encryption key based on the hashing encryption key K and the feedback hashed signal F which corresponds to the recited encrypted data).

As per claim 11, Meaden discloses:

The method of claim 10 wherein the step of encrypting a data record with a hash vector based upon an encryption key comprises performing a logic operation on a data record and a hash vector based upon an encryption key (see Fig. 1 and col. 4, lines 1-20, where the XOR operation is a logic operation).

As per claim 12, Meaden discloses:

The method of claim 11 wherein the step of performing a logic operation on a data record and a hash vector based upon an encryption key comprises performing an XOR operation on a data record and a hash vector based upon an encryption key (see Fig. 1 and col. 4, lines 1-20, where the XOR operation is a logic operation).

As per claim 13, Meaden discloses:

The method of claim 10 further comprising the step of decrypting encrypted data, comprising performing a logic operation on an encrypted data record and a hash vector based upon an encryption key (see Fig. 1, where the output data from gate 25 corresponds to the recited encrypted data and the feedback hashed signal F corresponds to the recited hash vector and col. 4, lines 1-20, where the XOR operation is a logic operation).

As per claim 14, Meaden discloses:

The method of claim 13 wherein the step of performing a logic operation on an encrypted data record and a hash vector based upon an encryption key comprises performing an XOR operation on an encrypted data record and a hash vector based upon an encryption key (see Fig. 1, where the output data from gate 25 corresponds to the recited encrypted data and the feedback hashed signal F corresponds to the recited hash vector and col. 4, lines 1-20, where the XOR operation is a logic operation).

Allowable Subject Matter

Claim 4 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (see attached PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Abdulhakim Nobahar/
Examiner, Art Unit 2132

April 26, 2008

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132